REMARKS

Claim Rejections – 35 USC §112

Withdrawal of the previous rejection under § 112 is acknowledged and appreciated.

Claim Rejections – 35 USC §101

Withdrawal of the previous rejection of claims 1-7 under § 101 is acknowledged and appreciated.

Claims 31-34 are rejected under 35 USC §101 as being directed to non-statutory subject matter.

The amendment to independent claim 31 should alleviate any subject matter issue with claims 31-35.

Double Patenting

Claims 7, 23, and 31 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1, 13 and 20 of copending application number 10/006,465.

A terminal disclaimer in compliance with 37 CFR 1.321 accompanies this rejection and should overcome this basis of rejection.

Claim Rejections – 35 USC §102

Claims 16-22 are rejected under 35 USC §102(e) as being anticipated by U.S. Patent 6,865,431 to Hirota et al. ("Hirota").

Independent claim 16 is reproduced below.

16. (Previously Amended) A method of playing encrypted audio or video content stored in a secure media with a device, the method comprising:

a pre-play process comprising:

copying one or more groups of information regarding the tracks to be played back into a memory of the device; and

a play process comprising:

receiving one more commands from a user interface to initiate playback;

accessing the one or more groups of information from the memory of device;

copying approximately less than one to five seconds of encrypted content from the secure media into a memory of the device according to a sequence based upon information of the one or more groups of information copied into the ram memory; and

decrypting the approximately less than one to five seconds of encrypted content before copying and decrypting an additional approximately less than one to five seconds of content.

The Examiner asserts that Hirota teaches "copying approximately less than one to five seconds of encrypted content from the secure media into a memory of the device according to a sequence based upon information of the one or more groups of information copied into the ram memory" (col. 59, line 53 – col. 60 line 11) and decrypting the approximately less than one to five seconds of encrypted content before copying and decrypting an additional approximately less than one to five seconds of content (col. 15, lines 45-53; col. 42, lines 34-35; col. 60, line 11)."

It is respectfully asserted that Hirota does not teach at least the limitations of independent claim 16 that recite "copying ... and decrypting the approximately less than one to five seconds of encrypted content before copying and decrypting an additional approximately less than one to five seconds of content".

While it is true that Hirota discloses the *playback time* of an AOB element will be around two seconds, as cited by the Examiner (Col. 15 line 45-53), Hirota does not teach "copying ... and decrypting the approximately less than one to five seconds of encrypted content before copying and decrypting an additional approximately less than one to five seconds of content." Col. 15 line 45-53 of Hirota, as cited by the Examiner, is reproduced below.

An "AOB_ELEMENT" is a group of consecutive AOB_FRAMEs. The number of AOB_FRAMEs in an AOB_ELEMENT depends on the value set as the sampling_frequency_index shown in FIG. 11A and the encoding method used. The number of AOB_FRAMEs in an AOB_ELEMENT is set so that the total playback time of the included AOB_FRAMEs will be around two seconds, with this number depending on the sampling frequency and encoding method used.

Hirota is silent on the quantity of content (measured in a decrypted and decoded format) that is copied and decrypted before copying and decrypting an additional quantity. Although

Hirota appears to be silent on this issue, if any of the disclosure within Hirota could be interpreted to teach or suggest a quantity copying and decrypting, the suggestion would appear to be a much larger quantity, the amount of content contained within a complete AOB file. Hirota teaches, "a descrambler 7 for decrypting AOB_FRAMEs *using a different FileKey for each AOB file*." Col. 42, lines 34-36. See also eg. FIG. 8A, FIG. 8B, FIG. 9, and FIG. 10. This AOB file is believed, as far as can be ascertained, to comprise many AOB elements and to correspond to an entire track or part of a very long track (if the track is too long/large to be comprised of only one AOB file). Thus, while Hirota appears silent on the amount of quantity copied and decrypted, or alternatively suggests that an entire file worth of content is decrypted at once, one thing is clear: it does not teach the claim 16 recitations of "copying … and decrypting the approximately less than one to five seconds of encrypted content before copying and decrypting an additional approximately less than one to five seconds of content." In summary, Hirota does not teach any type of cyclical copying and decrypting of small chunks, let alone doing so as part of playback process in order to limit exposure of the encryption keys.

Thus, Hirota does not teach all of the elements of independent claim 16 and cannot anticipate claim 16 and the claims that depend therefrom. It is therefore submitted that claims 16-22 are in condition for allowance.

Claim Rejections – 35 USC §103

Claims 4-7 and 24-29 are rejected under 35 USC §103(a) as being unpatentable over Hirota in view of U.S. Patent 6,615,192 to Tagawa et al. ("Tagawa"). Note that this should not be confused with other patents to Tagawa et al.

Independent claim 4 is reproduced below.

4. (Previously Amended) A computer readable storage medium having an executable program, the program to be utilized in an audio and/or video device for playback of encrypted audio and/or video files, the program configured to:

decrypt encrypted audio and/or video content of the file from a memory card based on a command received from a user interface of the device, wherein decrypting the audio or video content comprises:

copying one or more encrypted keys from a protected area of the memory card into a memory buffer of the device;

copying encrypted audio or video content from the memory card into a memory buffer of the device;

decrypting one or more of the copied encrypted keys;

decrypting the copied encrypted audio or video content with the one or more decrypted keys; and

immediately deleting the one or more decrypted keys after decrypting the audio and/or video content before decrypting additional content of the file.

The Examiner indicates that "Hirota does not explicitly disclose immediately deleting the one or more keys after decrypting the audio and/or video content before [decrypting] additional content of the file" but that Tagawa "discloses immediately deleting the one or more keys after decrypting the audio and/or video content before [decrypting] additional content of the file." Office action at page 8. The Examiner cites Col. 8, lines 56-61 and Col. 11, lines 32-33 of Tagawa for this proposition.

It is respectfully asserted that Tagawa does not teach such a thing, where cited by the Examiner or elsewhere. Tagawa does not teach "decrypting one or more of the copied encrypted keys." The recited copied encrypted keys are previously copied to a buffer of a playback device in antecedent limitations of the claim before they are deleted. Tagawa does not such a key and the recited usage thereof. Furthermore, Tagawa does not teach or suggest "immediately deleting one or more decrypted keys after decrypting the audio and/or video content before decrypting additional content of the file." Nothing in Tagawa teaches or suggests a file that is partially decrypted *before decrypting additional content of the file*. Nor does it teach or suggest that the key necessary to do so (which was previously copied into the device in encrypted state and then decrypted) is immediately deleted before decrypting additional content of the file.

To the contrary, Tagawa, at Col. 8, lines 56-61, and Col. 11, lines 32-33, as cited by the Examiner, appears to teach, if anything, that a "title key" is only deleted "after copying is performed by the disc drive 2" (Col. 11, line 22) and that "title and disc keys must be obtained anew from the DVD-Audio disc each time the user wishes to make a copy, so that the user must have the original DVD-Audio disc in order to be able to make copies" (Col. 11, lines 34-37).

Additionally, it does not appear that Tagawa even teaches the disclosed key is first copied in an encrypted state, and then decrypted, which is required by the antecedent limitations of the claim.

Furthermore, even if the combination of Hirota and Tagawa did teach all the limitations of claim 4, one of skill in the art would not be motivated to make such a combination.

First, as a threshold matter, one of skill in the art would not look to Tagawa in solving the particular problem at hand. Tagawa relates to limiting copies of DVD Audio discs. Claim 4 recites "A computer readable storage medium having an executable program, the program to be utilized in an audio and/or video device for playback of encrypted audio and/or video files." Tagawa does not relate to an executable program to be utilized for **playback** of encrypted audio and/or video files. Tagawa is very focused upon and relates almost entirely to making copies and more specifically to preventing a copy of DVD Audio disc made with a computer from being copied yet again. In summary, its teachings relate to prohibiting making a copy of a copy of the original disc. This is not pertinent to claim 4 or the other claims and teachings of the application. One of skill in the art would therefore not look to Tagawa, and it cannot therefore properly form the basis of a §103 rejection.

Second, there are no specific teachings in either Hirota or Tagawa that would lead one of skill in the art to combine the teachings of the references to arrive at the invention recited in claim 4. Nor has the Examiner cited any specific teachings that would lead one of skill in the art to combine Hirota and Tagawa. The Examiner indicates that "it would have been obvious to a person having ordinary skill in the art at t the time the invention was made to modify the method disclosed by Hirota with Tagawa in order to minimize the damage caused by the exposure of one of the encryption keys." Office Action at page 8. It is respectfully asserted that there is nothing in Tagawa that teaches exposed (decrypted keys passed in a vulnerable state) encryption keys. In fact, the solution advocated by Tagawa does not appear to copy the cipher key. See e.g. Tagawa Title "...disc drive copying contents but not a cipher key via a host computer."

Independent claim 24 is reproduced below.

24. (Previously Amended) A method for allowing a device having a processor and random access memory to easily access encrypted data from a memory card with a group of commands, the method comprising:

retrieving playlist information from the memory card and storing the information in the random access memory of the device;

retrieving track information from the memory card and storing the track information into the random access memory of the device;

receiving a command selected from the group of commands from the device, the command accessing both of the playlist information, and track information from the random access memory; and

executing the command by retrieving the encrypted data stored within the memory card and decrypting the data based on the accessed information, wherein decrypting the data comprises,

(a) calculating a media unique key; and thereafter

(b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter

(c) decrypting a group of frames; and thereafter

(d) deleting the decrypted title key;

(e) deleting the media unique key; and

(f) repeating (a) through (e) until the entire track is completed.

Claim 24 stands rejected based primarily upon Hirota and the Examiner admits that "Hirota does not explicitly disclose (d) deleting the decrypted title key; and (e) deleting the media unique key," and therefore relies on Tagawa for these teachings and asserts that "Tagawa, in analogous art, however, discloses the title and disc key may be deleted whenever copying is performed. (Col. 8, 56-61; Col. 11, lines 32-33). Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Hirota with Tagawa in order to minimize the damage caused by the exposure of one of the encryption keys. (col. 4, 17-19; Hirota)." Office Action at page 10.

It is kindly asserted that the combination of Hirota and Tagawa does not teach all of the elements of independent claim 24, as will be discussed below. It therefore cannot render the claim obvious.

Tagawa is cited for the proposition of teaching of steps (d) and (e) of the claim. Steps (d) and (e) are steps of an overall process of decrypting a track. Tagawa simply does not teach

those steps, as will be discussed below. Further, it is well known that patentable combinations and processes often comprise individual elements or steps that may individually also be well known in the art. Even if the steps, taken individually, are well known, this does not render the combination as a whole obvious.

The relevant portion of Tagawa, as cited by the Examiner, relates to limiting copies of DVD Audio discs. It discloses a way to prevent a copy of DVD Audio disc made with a computer from being copied yet again. In summary, it prevents making a copy of a copy of the original disc. This is apparently done by deleting the title and disc keys so they are not written to the first copy of the DVD Audio disc. Therefore, a subsequent copy is prevented by a user who does not possess the original disc. The relevant portion of Tagawa is reproduced below.

> Title and disc keys stored in the EEPROM 23 are deleted by the control microcomputer 26 when the limit set for the number of copies 1108 has been reached. Alternatively, the title and disc keys may be deleted whenever copying is performed by the disc drive 2. In the latter case, the title and disc keys must be obtained anew from the DVD-Audio disc each time the user wishes to make a copy, so that the user must have the original DVD-Audio disc in order to be able to make copies. As a result, copying by a user who does not possess an original disc can be prevented even if the number of copies has not reached its limit, and only copying made by the user in possession of the original disc authorized. Tagawa Col. 11, line 29-41.

This is not relevant to the process recited in claim 24 wherein:

> decrypting the data comprises,
> (a) calculating a media unique key; and thereafter
> (b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter
> (c) decrypting a group of frames; and thereafter
> (d) deleting the decrypted title key;
> (e) deleting the media unique key; and
> (f) repeating (a) through (e) until the entire track is completed.

Similarly to the discussion of independent claim 4 above, Tagawa, alone or in combination with Hirota, does not teach at least " (c) decrypting a group of frames; and thereafter (d) deleting the decrypted title key; (e) deleting the media unique key; and

(f) repeating (a) through (e) until the entire track is completed." Tagawa simply does not teach such an iterative process performed "until the entire track is completed," alone or in combination with Hirota.

Furthermore, it is unclear in the rejection of any of the claims that recite a media unique key that the same media unique key exists in all of the references of the combination. There is nothing indicating that the disc key of Tagawa is the same as or equivalent to the media unique key asserted to be taught by Hirota.

Independent claim 7 stands rejected upon the same basis as independent claim 24, and is in condition for allowance for reasons given regarding claim 24. Therefore, it is kindly submitted that claims 4-7 and 24-29 are in condition for allowance.

Claims 23 and 31-34 are rejected under 35 USC §103(a) as being unpatentable over Hirota in view of Tagawa and in view of U.S. Patent 6,615,195 to Saxena et al. ("Saxena").

Independent claim 23 is reproduced below.

23. (Original) A system enabling a portable device to access encrypted music on a memory storage device comprising:
one or more application programming interfaces configured to:
receive a plurality of commands from a user interface of the portable device; and
send commands to an isolated security engine, the isolated security engine configured to:
receive commands from the application programming interface;
copy encrypted keys and encrypted content from the memory storage device to a memory of the portable device;
decrypt the keys;
decrypt the content using the decrypted keys; and thereafter
delete the decrypted keys.

As admitted by the Examiner, the combination of Hirota and Tagawa does not teach "an applications programming interface for receiving the commands from the one or more user interface modules and managing the retrieval and storage of encrypted content from the secure medium." Therefore, the Examiner has added Saxena to the combination of Hirota and Tagawa.

There is no teaching of encryption or decryption with Saxena. Thus, Saxena cannot and does not teach "one or more application programming interfaces configured to:...copy encrypted

keys and encrypted content from the memory storage device to a memory of the portable device; decrypt the keys; decrypt the content using the decrypted keys; and thereafter delete the decrypted keys." The simple disclosure of an API within Saxena (a portion of which are reproduced below) does not teach the claim limitations regarding to the specific API of the claim.

While Saxena does disclose usage of an API, Saxena is not related to and does not teach "a system enabling a portable device to access encrypted music on a memory storage device." Usage of such an API is not trivial, and serves to enable the system to work with a variety of different devices that may have completely different user interfaces and hardware/software platforms. The API enables one system to work in a myriad of different hardware/software platforms to retrieve content from a media storage device, which in the preferred embodiments is a portable memory card. This is very different than the teachings of Saxena which relate to streaming content over a network.

> The system of this invention provides the following features: scaleability to deliver from 1 to 1000's of independently controlled data streams to end users; an ability to deliver many isochronous data streams from a single copy of data; mixed output interfaces; mixed data rates; a simple "open system" control interface; automation control support; storage hierarchy support; and low cost per delivered stream. Saxena Summary.

Even if the combination of Saxena, Hirota and Tagawa does teach all of the recitations of the claim, one of skill in the art would not be motivated to combine all of the three references. Saxena is not pertinent to the "system enabling a portable device to access encrypted music on a memory storage device" recited in claim 23, but instead relates to a video optimized media streamer user interface employing non-blocking switching to achieve isochronous data transfers. While Saxena mentions usage of an API, this is an insufficient motivation to combine. There are no specific teachings with the references that would lead one of skill in the art to combine the teachings of all three of these references to arrive at the claimed combination. As mentioned above, Saxena is related to and teachings streaming thousands of data streams to end users, not to the claimed system. Furthermore, as mentioned earlier, Saxena has no teachings related to encryption or decryption of content and/or keys.

Independent claim 31 is reproduced below.

31. (Currently Amended) A software system stored on a device that enables the device to access content on a secure medium comprising:

one or more user interface modules for receiving commands from the device;

an applications programming interface for receiving the commands from the user interface module(s) and managing the retrieval and storage of both encrypted and non encrypted content from the secure medium;

a security engine for decrypting the encrypted content and encrypted keys sent from the secure medium to memory of the device, the decrypted keys used to decrypt the encrypted content, and wherein

one or more of the keys are contained in a first encrypted data segment, and encrypted content is contained in a second encrypted data segment, and

the security engine buffers and decrypts a portion of the first data segment, buffers and decrypts the second data segment, and thereafter deletes the decrypted one or more keys before decrypting another portion of the first encrypted data segment, such that decrypted keys are in a decrypted state for the time it takes to decrypt less than one to about five seconds of content.

The combination of Hirota, Tagawa, and Saxena fails to teach at least the following limitations of claim 31 wherein "one or more of the keys are contained in a first encrypted data segment, and encrypted content is contained in a second encrypted data segment, and the security engine buffers and decrypts a portion of the first data segment, buffers and decrypts the second data segment, and thereafter deletes the decrypted one or more keys before decrypting another portion of the first encrypted data segment, such that decrypted keys are in a decrypted state for the time it takes to decrypt less than one to about five seconds of content."

In particular, Col. 12 lines 1-12, cited by the Examiner, appears to be teaching about content, not keys. The cited portions of Columns 9 and 41 discuss file keys, but never teach that "the security engine buffers and decrypts a portion of the first data segment, buffers and decrypts the second data segment, and thereafter deletes the decrypted one or more keys before decrypting another portion of the first encrypted data segment, such that decrypted keys are in a decrypted state for the time it takes to decrypt less than one to about five seconds of content."

Therefore, it is kindly submitted that claims 23 and 31, and all the claims that depend therefrom, are in condition for allowance.

Conclusion

Accordingly, it is believed that this application is now in condition for allowance and an early indication of its allowance is solicited. However, if the Examiner has any further matters that need to be resolved, a telephone call to the undersigned attorney at 415-318-1163 would be appreciated.

FILED VIA EFS

Respectfully submitted,

Gerald P. Parsons
Reg. No. 24,486

11/9/06
Date

PARSONS HSUE & DE RUNTZ LLP
595 Market Street, Suite 1900
San Francisco, CA 94105
(415) 318-1160 (main)
(415) 318-1163 (direct)
(415) 693-0194 (fax)